IN THE CLAIMS:

This listing of claims will replace all prior versions, and listing, of claims in the application.

Listing of the Claims:

1. (Original) A method of communicating an electronic document between security domains, the method comprising the steps of:

receiving, in a first security domain, a request to transmit to a second security domain a first electronic document in a first data format capable of supporting one or more (covert) security threats;

creating a second document in a second data format incapable of supporting the one or more security threats, responsive to the content of the first document;

forwarding the second document in place of the first document to the second security domain.

2. (Currently amended) A method according to ~~any preceding~~ claim 1 in which forwarding of the second document is conditional upon user sanction.

3. (Currently amended) A method according to ~~any preceding~~ claim 1 in which the second document is digitally signed by a sanctioning user.

4. (Currently amended) A method according to ~~any preceding~~ claim 1 in which the second document is forwarded to the second security domain via at least one data diode.

5. (Currently amended) A method according to ~~any preceding~~ claim 1 in which the step of creating the second document comprises performing a transformation to the first

document which modifies the underlying data format of the document whilst substantially preserving the visible informational content.

6. (Currently amended) A method according to ~~any preceding~~ claim 1 in which the step of creating the second document comprises adding at least one of entropy and randomness to at least one characteristic of the representation of the first document.

7. (Original) A method according to claim 6 in which the at least one characteristic comprises at least one of colour and spacing.

8. (Currently amended) A method according to ~~any preceding~~ claim 1 in which the step of creating the second document comprises applying a lossy compression method.

9. (Currently amended) A method according to ~~any preceding~~ claim 1 comprising the step of:

conveying the second document to a user sanction function for review and sanction prior to sending the second document to the second security domain.

10. (Currently amended) A method according to ~~any preceding~~ claim 1 in which review and sanction comprises sanction by a human user.

11. (Currently amended) A method according to ~~any preceding~~ claim 1 in which the one or more security threats comprise presence in the first document of malicious code.

12. (Original) A method according to claim 11 in which the malicious code comprises at least one of a computer virus and a Trojan horse.

13. (Currently amended) A method according to ~~any preceding claims~~ claim 1 in which the one or more security threats comprises data steganographically concealed within the first document.

14. (Currently amended) A method according to ~~any preceding~~ claim 1 in which the first security domain and second security domain are rated at different security levels.

15. (Currently amended) A method according to ~~any preceding~~ claim 1 in which the first security domain is a lower-level security domain than the second security domain.

16. (Currently amended) A method according to ~~any one of claim 1-14~~ claim 14 in which the first security domain is a higher-level security domain than the second security domain.

17-21. (Cancelled)

22. (New) Apparatus for communicating an electronic document between security domains, the apparatus comprising:

apparatus arranged to receive, in a first security domain, a request to transmit to a second security domain a first electronic document in a first data format capable of supporting one or more (covert) security threats;

apparatus arranged to create a second document in a second data format incapable of supporting the one or more security threats, responsive to the content of the first document;

apparatus arranged to forward the second document in place of the first document to the second security domain.

23. (New) A computer chipset for communicating an electronic document between security domains, the computer chipset comprising:

a first component arranged to receive, in a first security domain, a request to transmit to a second security domain a first electronic document in a first data format capable of supporting one or more (covert) security threats;

a second component arranged to create a second document in a second data format incapable of supporting the one or more security threats, responsive to the content of the first document;

a third component arranged to forward the second document in place of the first document to the second security domain.

24. (New) A computer readable medium having program code record thereon to direct a computer to communicate an electronic document between security domains, the program comprising:

a first code portion arranged to receive, in a first security domain, a request to transmit to a second security domain a first electronic document in a first data format capable of supporting one or more (covert) security threats;

a second code portion arranged to create a second document in a second data format incapable of supporting the one or more security threats, responsive to the content of the first document;

a third code portion arranged to forward the second document in place of the first document to the second security domain.